

El malware nuestro de cada día

(short version)

Lucas González • 05.08.2020



No estás solo

REvil ransomware infected 18,000 computers at Telecom Argentina

July 20, 2020 By Pierluigi Paganini

Another telco company was hit by a ransomware, roughly 18,000 computers belonging to Telecom Argentina were infected over the weekend.

Telefonica, other Spanish firms hit in "ransomware" attack

4 MIN READ



MADRID (Reuters) - Spain said on Friday a large number of companies, including telecommunications giant Telefonica ([TEF.MC](#)), had been infected with malicious software known as "ransomware" which locks up computers and demands ransoms.

CSIRT-NQN Retweeted



CSIRT-CV @CSIRTCV · Jan 24

Expuestos 250 millones de registros de #Microsoft. Una brecha de seguridad afecta a los registros de asistencia al cliente de Microsoft. La causa, una errónea configuración en las reglas de seguridad de un servidor.

Más detalles: ow.ly/X54I30qbXre



News

Garmin confirms ransomware cyberattack shut down services

By **Zoe Christen Jones**

July 27, 2020

Áreas Específicas

amazon.jobs/en/business_categories/amazon-web-services

Q | 0¹³ A

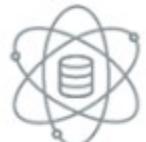
Search Jobs



Administrative
Support



Business
Development



Data Science



Design



Hardware
Development



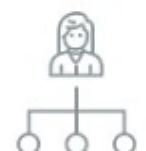
Machine
Learning



Marketing



Product
Management



Program
Management



Sales



Security Engineer



Software
Development
Engineer



Solutions
Architect



Support Engineer



System
Development
Engineer

Áreas Específicas

Security Engineer- AWS Fraud

Job ID: 968185 | Amazon Web Services, Inc.

Sr. Security Engineer- AWS Fraud Prevention

Job ID: 968184 | Amazon Web Services, Inc.

Security Engineer, Elastic Compute Cloud (EC2)

Job ID: 960730 | Amazon Dev Center U.S., Inc.

Senior Security Engineer - Hardware

Job ID: 979735 | Amazon.com Services LLC

Security Engineer, Research and Automation, AWS

Job ID: 997198 | Amazon Web Services, Inc.



Bienvenido: Hombre Orquesta

- Administradores Locales de GDE
- Impresoras
- Soporte al Usuario
- Soporte a Usuarios Especiales ;)
- Administrar Servidores
- Actualizar Equipos
- Reparar Equipos
- UPS
- Venderle a Usuarios Especiales que compre licencias, por ejemplo.
- Llevarle facturas y mates a Compras
- Que nos compren lo que realmente pedimos
- Documentar lo que hacemos
- Revisar Dasboards
- ¡Ah! Seguridad También...
- Etc ¡Uff!

Necesitamos una Metodología de Trabajo



1° Consolidar, Monitorear y Defender Gateways



Controlar lo que sale y entra de tu red.

Fácil es decirlo: ¿Cómo lo hacemos?

- 1) Herramientas de Monitoreo (Gratuitas), veamos algunas.**
- 2) Administrar nuestros Gateways.**

- **Para eso Necesitamos un Router (veamos)**
- **Si no nos compran, una PC con Dos Placas de Red (veamos)**

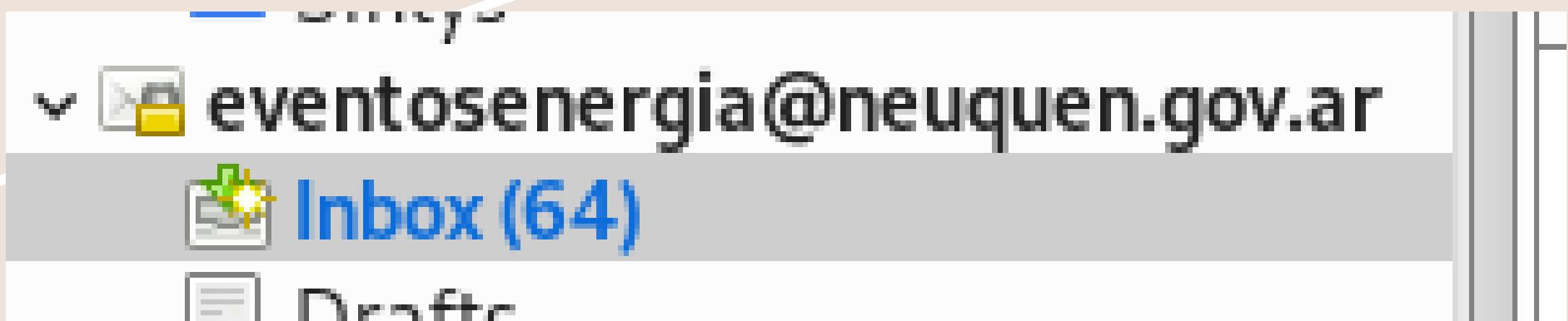
¡No todo Brilla en Babilonia!

1) Incrementamos Dispositivos.

- ¿Dónde están tus dispositivos?
- ¿Cuántos dispositivos tenemos?
- ¿Quién los administra?

2) Monitoreo y Logs

- ¿Quién los mira?



¡No todo Brilla en Babilonia - 1!

“When **alerts are more often false than true**, the on-call’s sense of urgency in responding to alerts is diminished ... the simple burden of alerts **desensitizes the on-call to alerts.**”

2º Parchear y Actualizar OS y Aplicaciones



- Tener Sistemas de Actualización**
- Fácil es decirlo: ¿Cómo lo hacemos?
- 1) WSUS - > OBLIGATORIO**
 - 2) Herramientas de Terceros**
 - **Actualizar Mediante Endpoints**

No todo Brilla en Babilonia - 3

Equipos

Esta vista muestra un resumen del estado de los equipos por grupo de equipos.

Información general

Todos los equipos



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Equipos sin asignar



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Equipos con errores



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Equipos que necesitan actualizaciones



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Equipos instalados/no aplicables



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Equipos sin estado



■ Equipos con errores:	0
■ Equipos que necesitan actualizaciones:	0
■ Equipos instalados/no aplicables:	0
■ Equipos sin estado:	0

Acti

No todo Brilla en Babilonia - 4

Servidor de administración Dispositivos administrados Desktops

Dispositivos administrados

Dispositivos Directivas Tareas Propiedades del grupo Actualizar

Mover dispositivos al grupo Nuevo grupo Realizar acción ▾ Agregar/eliminar columnas

No se especificó un filtro, total de registros: 54 Buscar por columnas de texto

Seleccionar estados: Crítico: 14 Advertencia: 18 Sin inconvenientes: 22

El total de registros que se muestra arriba incluye el número de dispositivos que tienen el estado especificado y que pertenecen al grupo indicado o a cualquiera de sus subgrupos. La lista que se encuentra a continuación incluye solo los dispositivos del grupo seleccionado.

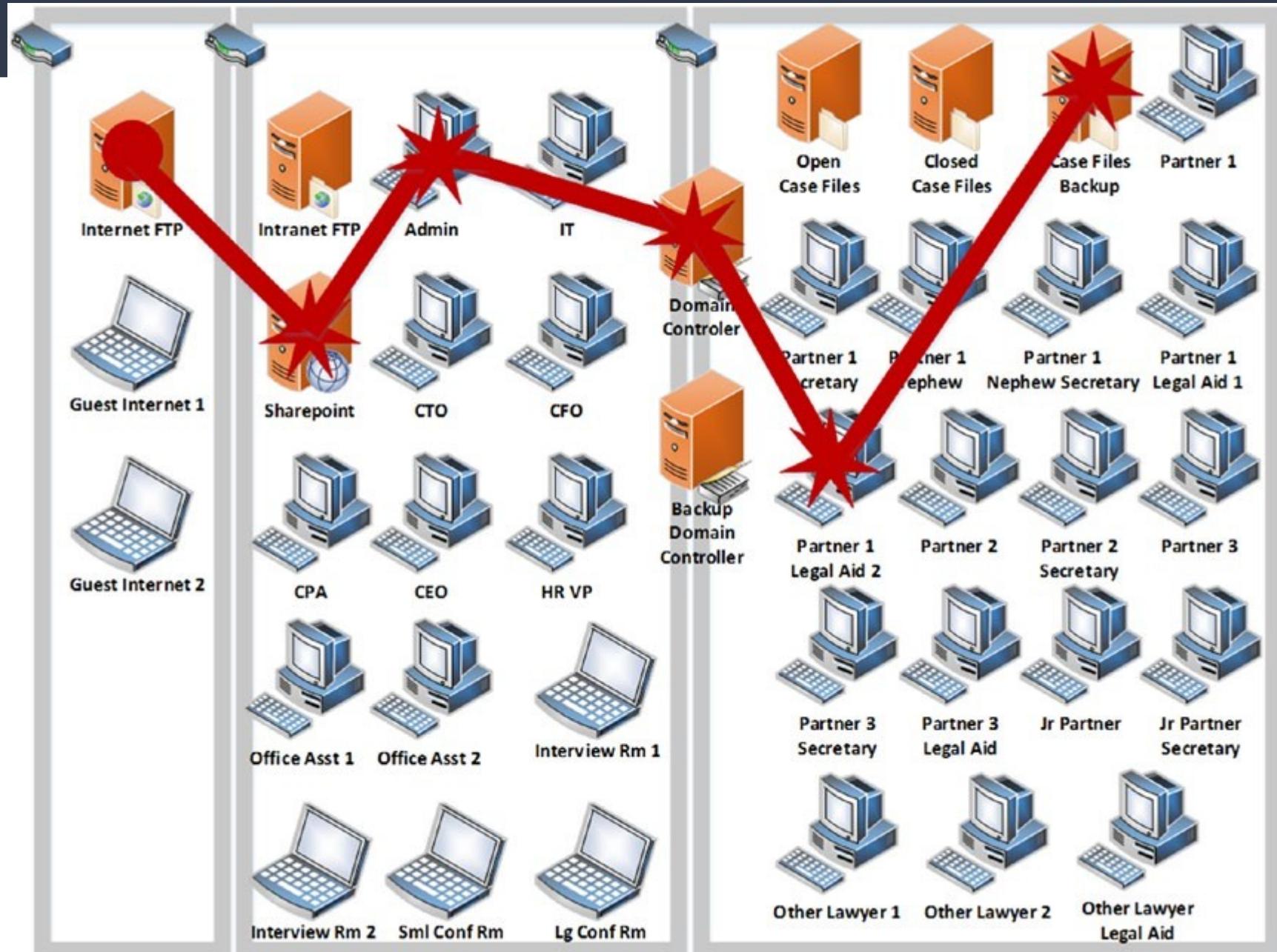
Nombre	Última conexión...	Agente de red ...	Estado de protección en tiempo real	Cre...
	Hace 2 horas	✓ Sí		19/0...
	Hace 3 semanas	✓ Sí		22/0...
	hace un día	✓ Sí		17/0...
	Hace 12 minut...	✓ Sí	En ejecución	11/0...
	Hace 10 minut...	✓ Sí	En ejecución	11/0...
	Hace 3 días	✓ Sí		17/0...
	Hace 1 semanas	✓ Sí		04/0...
	Hace 9 minutos	✓ Sí	En ejecución	17/0...
		! No		11/0...
	Hace 9 minutos	✓ Sí	En ejecución	17/0...
	Hace 45 minut...	✓ Sí	En ejecución	11/0...
		! No		11/0...
		! No		11/0...

Estado del dispositivo: Crítico
Se detectaron demasiados virus ▾

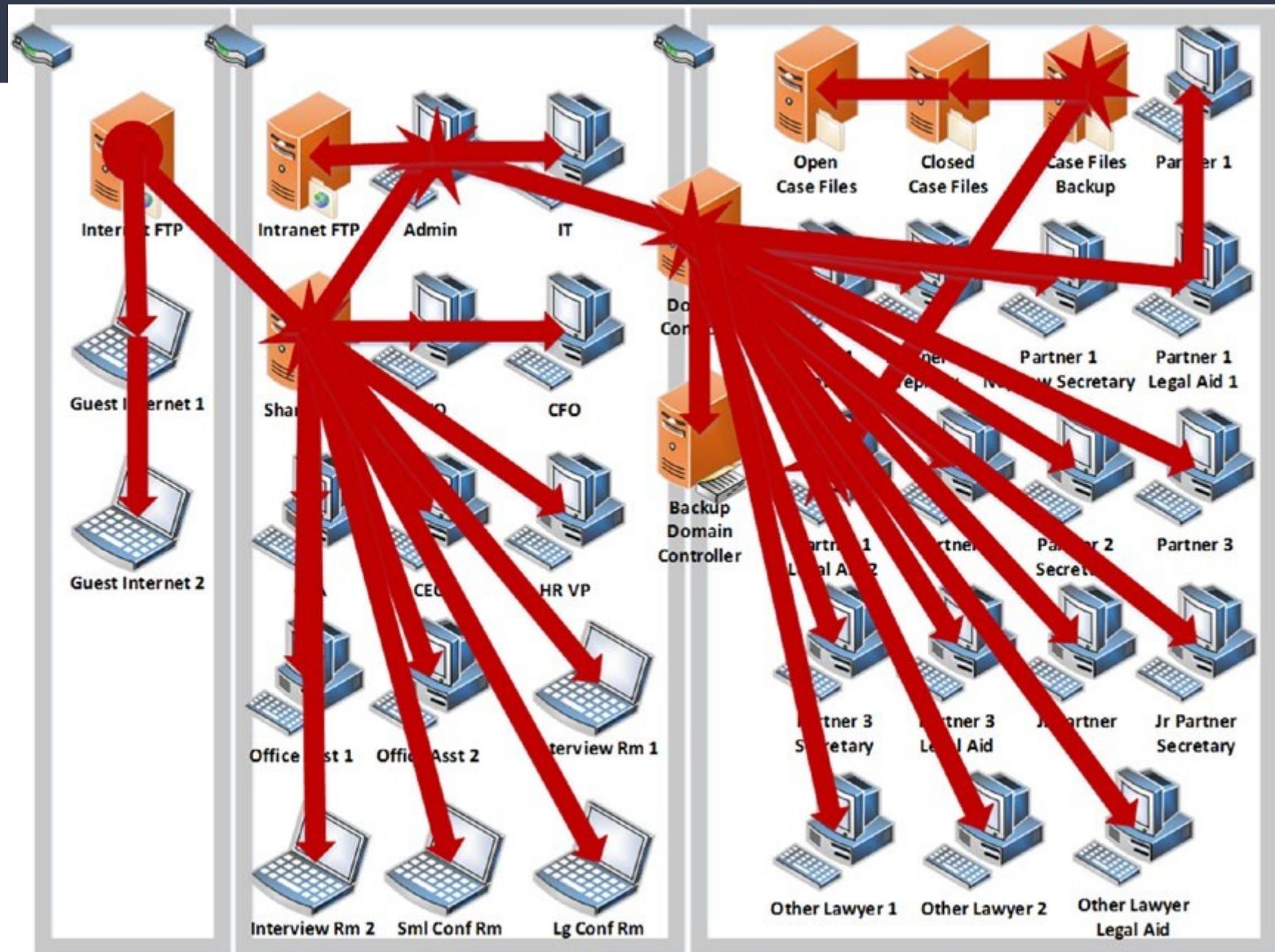
Se requiere reinicio. Motivo:
Se debe reiniciar el dispositivo para completar la actualización que está ejecutando la aplicación
Se requiere reiniciar para completar la instalación o la desinstalación remotas

Propiedades
Nombre de dominio
DNS:
Dirección IP:
Activar Windows Estado de protección No hay datos del dispositivo
Vaya a Sistema y activar Windows

Escalando Privilegios – Movimientos Laterales (Específico – Alguien lo paga...)



Escalando Privilegios – Movimientos Laterales (Como lo tenemos que pensar...)



Herramienta de Auditoría – 1



Buscar:

**Death star
domain admin**

Herramienta de Auditoría - 2 ;)



BLOODHOUND

Buscar:

**Bloodhound
domain admin**

Relax and drink wine...

**Vas a ver muchas cosas que no te
van a gustar...**



Bienvenido Mitre Attack...

attack.mitre.org

MITRE | ATT&CK® Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute

ATT&CK sub-techniques have now been released! Take a tour, read the blog post or release notes, or see the previous version of the site.

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK®

Getting Started Take a Tour

Contribute Blog

<https://attack.mitre.org/>

Tweets by @MITREattack

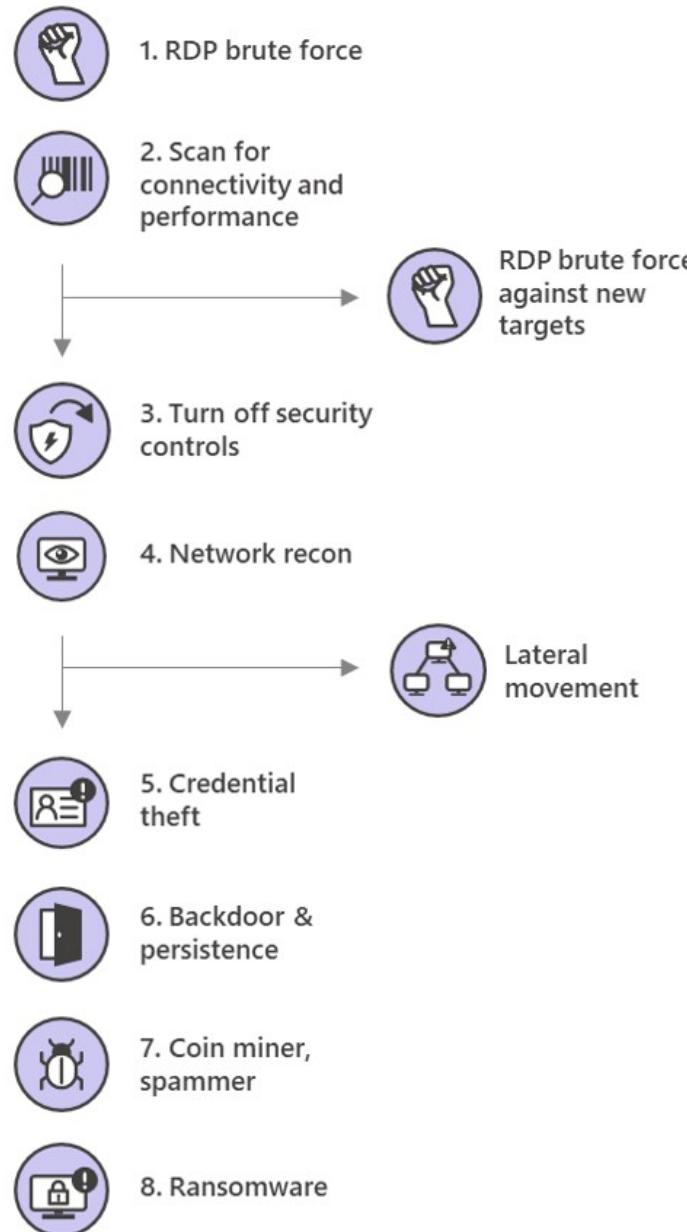
ATT&CK @MITREattack We've gotten a lot of questions about ATT&CKcon lately, and we're planing on doing something a bit different this fall. Stay tuned Monday for more details on ATT&CKcon Power Hour.



Embed View on Twitter

Mitre Attack...

Wadhrama attack chain



MITRE ATT&CK

T1076 | Remote Desktop Protocol

T1110 | Brute Force

T1089 | Disabling Security Tools

T1046 | Network Service Scanning

T1003 | Credential Dumping

T1136 | Create Account

T1219 | Remote Access Tools

T1060 | Registry Run Keys / Startup Folder

T1486 | Data Encrypted for Impact

Por donde se cuela el Malware – 1 (por todos lados)...



active processes. The attackers don't always install ransomware immediately; they have been observed installing coin miners and using *massmail.exe* to run spam campaigns, essentially using corporate networks as distributed computing infrastructure for profit. The group, however, eventually returns to the same machines after a few weeks to install ransomware.

Por donde se cuela el Malware

(por todos lados)...

Human-operated ransomware attacks



Common attack techniques



Initial entry through misconfigured or outdated web servers

- RDP brute force



Deployment through commodity malware infection

- Initial entry through Trickbot or Dridex



Finding and exploiting poor security controls

- Thorough reconnaissance to discover and leverage security weaknesses
- Extensive knowledge of system and network misconfigurations



Credential theft and escalation of privilege

- Credential dumping through tools like Mimikatz, ProcDump, or LaZagne
- Privilege escalation through Sticky Keys attack
- Theft of financial credentials and LSA secrets in registry
- Data exfiltration through RDP
- Creating new accounts then granting remote desktop privileges



Human-operated lateral movement

- Network recon through scanning tools
- Manual spread through PsExec and GPO



Disabling of security controls

- Stopping security services
- Clearing event logs

Defenses



Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials



Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise



Include IT Pros in security discussions

- Ensure collaboration among SecOps, SecAdmins, and IT admins to configure servers and other endpoints securely



Build credential hygiene

- Use MFA or NLA, and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege



Monitor for adversarial activities

- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events



Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and AMSI for Office VBA

TOP 16 - Vulnerabilidades Active Directory (seguimos contando...)

Top 16 Active Directory vulnerabilities

1. Users having rights to add computers to domain
2. AdminCount attribute set on common users
3. High number of users in privileged groups
4. Service accounts being members of Domain Admins
5. Excessive privileges allowing for shadow Domain Admins
6. Service accounts vulnerable to Kerberoasting
7. Users with non-expiring passwords
8. Users with password not required
9. Storing passwords using reversible encryption
10. Storing passwords using LM hashes
11. Service accounts vulnerable to AS-REP roasting
12. Weak domain password policy
13. Inactive domain accounts
14. Privileged users with password reset overdue
15. Users with a weak password
16. Credentials in SYSVOL and Group Policy Preferences (GPP)

3° - Reforzar la Gestión de Privilegios Administrativos



Usuarios Especiales



Usuarios especiales: Quieren Privilegios de Admin

Desarrolladores: Quieren Privilegios de Admin

Usuarios Especiales

si ya se que esta seteada para todos los usuarios, pero me parece que
nosotros informaticos no es necesaria la recomendacion, la quiero cambiar



Equipos de IT: Quieren Privilegios de Admin

¿Cuántos usan credenciales de Admin para entrar a sus DC u otros servidores?

No todo Brilla en Babilonia - 5

Te van a quedar pocos amigos...



No todo Brilla en Babilonia – 6

No viniste a hacer amigos...



**Un poco
(muy poquito)**

¿Consensuar?



Mucho



ACLight... Tu nuevo amigo...

```
ACLight2
ACLight2 - a tool for advanced discovery of Privileged Accounts - including risky Shadow Admins
Developed by Asaf Hecht (@Hechtov)
Uses functions from the great PowerView project (@harmj0y)
Follow Twitter for more future updates

Great, the scan was started - version 3.3.
It could take a while, (5-30+ mins) depends on the size of the network
Discovered [REDACTED] Domains

*****
Starting analysis for Domain: energianet [REDACTED] - Layer 1
Got more objects..
Finished scanning this layer in: 0.13 Minutes, 0.002 Hours
Scanning ACLs - Layer 2
Got more objects..
Finished scanning this layer in: 0.12 Minutes, 0.002 Hours
Scanning ACLs - Layer 3
Got more objects..
Finished scanning this layer in: 0.09 Minutes, 0.002 Hours
```

From direct ACL assignment:

Currently Shadow Admins were not detected in the network

Shadow Admins



Domain Admins Properties

General	Members	Member Of	Managed By
Object	Security	Attribute Editor	

Group or user names:

- MSOL_18453990b221
- Account Unknown(S-1-5-21-1858599162-3566974474-332785...)
- Account Unknown(S-1-5-21-1858599162-3566974474-332785...)
- Emily (Emily@research.com)
- Administrators
- Domain Admins (RESEARCH\Domain Admins)

Permissions for Domain Admins

	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

OK Cancel Apply Help

Domain Admins Properties

General	Members	Member Of	Managed By
Object	Security	Attribute Editor	

Group or user names:

- MSOL_18453990b221
- Account Unknown(S-1-5-21-1858599162-3566974474-332785...)
- Account Unknown(S-1-5-21-1858599162-3566974474-332785...)
- Emily (Emily@research.com)
- Administrators
- Domain Admins (RESEARCH\Domain Admins)

Permissions for Emily

	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

OK Cancel Apply Help

Group Assignment

VS

Direct Assignment

Domain Admins Properties

General	Members	Member Of	Managed By
Object	Security	Attribute Editor	

Group or user names:

- Exchange Trusted Subsystem (RESEARCH\Exchange Trusted ...)
- James (James@research.com)
- Domain Admins (RESEARCH\Domain Admins)
- Cert Publishers (RESEARCH\Cert Publishers)
- Enterprise Admins (RESEARCH\Enterprise Admins)
- Administrators (RESEARCH\Administrators)

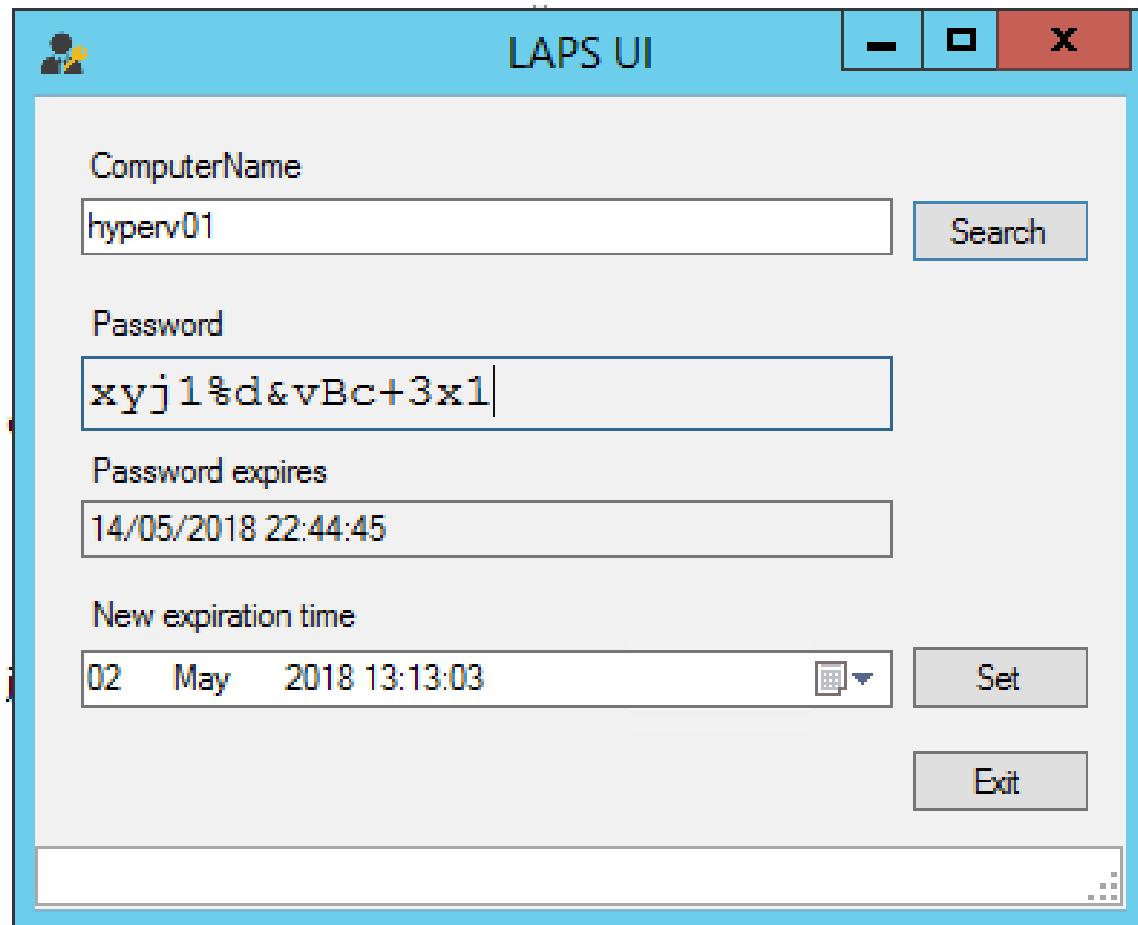
Permissions for James

	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>

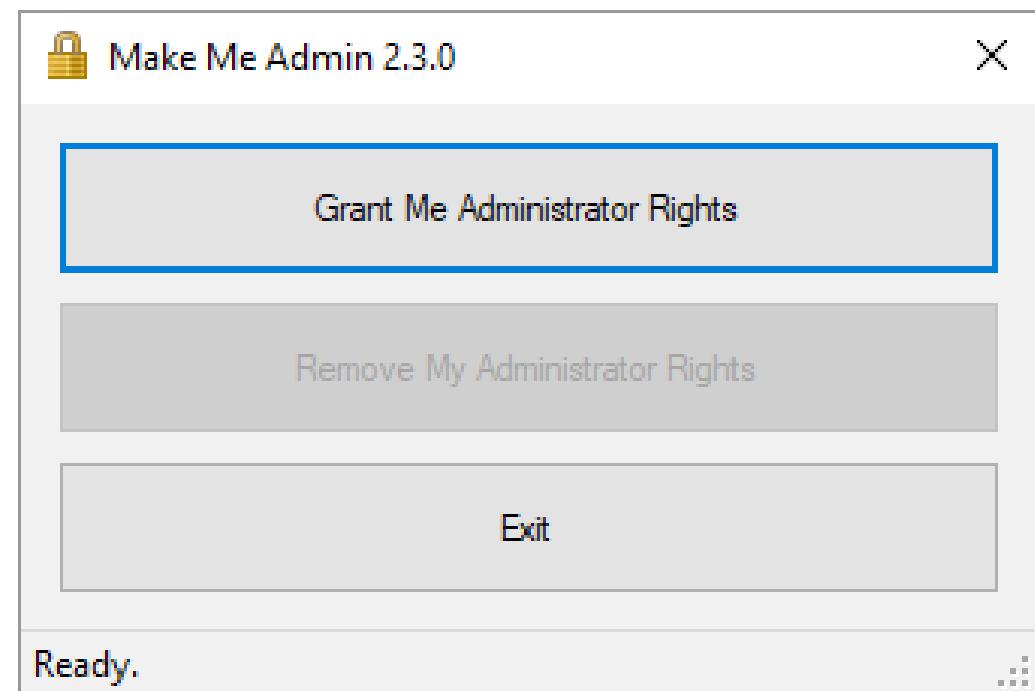
For special permissions or advanced settings, click Advanced.

OK Cancel Apply Help

Aplicarás LAPS



Make Me Admin



Para cortar tela...



AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

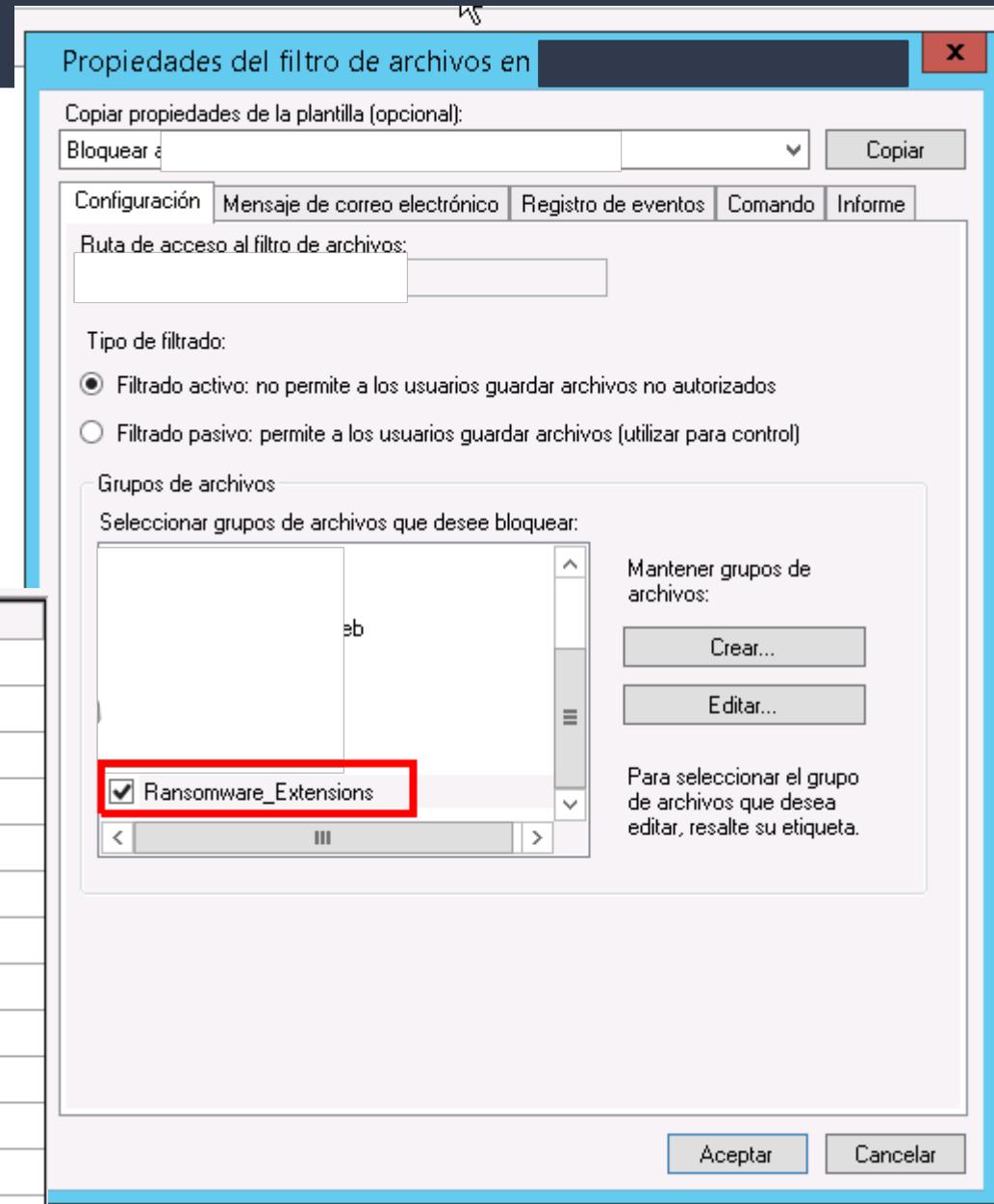
From Workstation to Domain Admin:
Why Secure Administration Isn't Secure and How to Fix It

<https://i.blackhat.com/us-18/Wed-August-8/us-18-Metcalf-From-Workstation-To-Domain-Admin-Why-Secure-Administration-Isnt-Secure.pdf>

Hablemos del Fileserver

- **En discos diferentes.**
- **En Servidores diferentes a DC (de ser posible)**
- **FSRM (File Server Resource Manager)**

Grupos de archivos	Incluir archivos	Excluir archivos
Archivos comprimidos	*.ace, *.arc, *.arj, *.bhx, *.bz2, *.ca...	
Archivos de audio y vídeo	*.aac, *.aif, *.aiff, *.asf, *.asx, *.au,...	
Archivos de copia de seguridad	*.bak, *.bck, *.bkf, *.old	
Archivos de correo electrónico	*.eml, *.idx, *.mbox, *.mbx, *.msg...	
Archivos de imagen	*.bmp, *.dib, *.eps, *.gif, *.img, *...	
Archivos de Office	*.accdb, *.accde, *.accdr, *.accdt,...	
Archivos de página web	*.asp, *.aspx, *.cgi, *.css, *.dhtml, ...	
Archivos de sistema	*.acm, *.dll, *.ocx, *.sys, *.vxd	
Archivos de texto	*.asc, *.text, *.txt	
Archivos ejecutables	*.bat, *.cmd, *.com, *.cpl, *.exe, *...	
Archivos temporales	*.temp, *.tmp, ~*	
Ransomware_Extensions	*.0x0, *.1999, *.CTB2, *.CTBL, *.En...	



¡Grandes dosis de Antivirus!



¿Cómo están
tus backups?
el día D, en algún
momento llega...



Cosas que callé

- MACROS (esos hdp...) Con suerte vas a poder quitarlos.
- SPF – DKIM
- GPOs (algunas son maliciosas...)
- Jump Boxes
- PingCastle
- LM – SMBv1 – NTLMv1 – Wdigest
- KRBTGT
- VLAN Rules – Rockstar
- Hardening Active Directory
- LSA Protection
- User Gropup Protection
- ASR – Attack Surface Reduction
- Etc...

Apicala...



¿A quién le toca
hacer todo esto?
Adivinaste...



¡Gracias!

lucasg@neuquen.gov.ar